UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,548	08/29/2000	Barry Atkins	RPS920000026US1	9903

42640 7590 01/26/2006

DILLON & YUDELL LLP
8911 NORTH CAPITAL OF TEXAS HWY
SUITE 2110
AUSTIN, TX 78759

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 01/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/651,548
Filing Date: August 29, 2000
Appellant(s): ATKINS ET AL.

ATKINS, BARRY
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/3/05 appealing from the Office action mailed 6/17/05.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,807,277	Doonan et al.	6-2000
6,009,177	Sudia, Frank Wells	2-1997
6,732,101	Cook, David P.	6-2000
4,888,800	Marshall et al.	3-1988

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-24 which is presented for examination. These rejections are set forth in prior Office Action, Paper No. 09651548\20050612 and reproduced for convenient.

Claim Rejection – 35 USC § 103

1. Claims 1 - 3, 6 - 11, 14 - 19, 22 - 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doonan et al. (US Patent No. 6,807,277) in view of Sudia (US Patent No. 6,009,177).

Regarding Claims 1, 9, 17 (currently amended), Doonan discloses a network messaging system. (see Doonan col. 1, lines 10-12: " ... *present invention is directed to*

a secure electronic messaging system ... ") Doonan discloses a method, a system and program product for managing a user key used to sign a message for a data processing system, said method comprising:

a) assigning a user key to a user and storing the user key in an encrypted data processing system utilized to encrypt messages; (see Doonan col. 2, lines 1-7: encryption key assigned by key server for message encryption)

b) encrypting the messages with the user key; (see Doonan col. 2, lines 7-8: message is encrypted)

c) storing an associated key in the encrypting data processing system and encrypting the user key with the associated key to obtain an encrypted user key; (see Doonan col. 5, lines 63-67: generate an encrypted user key for transmission)

d) said encrypting data processing system communicating at least one encrypted messages together with the encrypted user key to a recipient system in order to permit validation of an association of the user with the encrypted messages by the recipient system; (see Doonan col. 6, line 1: encrypted message and encrypted key are transmitted to recipient)

f) computer usable media bearing said control program. (see Doonan col. 3, lines 9-12; col. 9, lines 33-44: software exists on computer readable medium for program execution)

e) Doonan discloses a check on the validation of a sender's credentials. (see Doonan col. 5, lines 16-20: sender credentials are verified) Doonan does not

specifically disclose using a certificate authority (trusted third party) for key validation and determination of key revocation. However, Sudia discloses preventing validation of the association of the user with messages by revoking the associated key at the encrypting data processing system (see Sudia col. 22, lines 51-63; col. 23, lines 4-7: access revocation list to determinate whether certificate (attached key) is valid)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to invalidate the association key when the status of the association key has been revoked as taught by Sudia. One of ordinary skill in the art would be motivated to employ Sudia in order to enable a trusted third party for a flexible and independent network key management system. (see Sudia col. 10, lines 23-25: " ... *provide a commercial key escrow system that uses private keys that may be changed by the user at will or at regular intervals ...* "; col. 11, lines 15-23: " ... *a system of certificate management ... very flexible and independent of location and time ... escrowing a private decryption key and receiving an escrow certificate ... registering a trusted device with a trusted third party and receiving authorization from that party enabling the device to communicate with other trusted devices ...* ")

Regarding Claims 2, 10, 18 (original), Doonan discloses the method, system and program product according to Claims 1, 9, 17, further comprising:

a) decrypting the user key with the associated key; (see Doonan col. 6, lines 1-3: encrypted key is decrypted)

b) decrypting the messages with the user key. (see Doonan col. 6, lines 1-3: encrypted message is decrypted)

Regarding Claims 3, 11, 19 (currently amended), Doonan discloses the method, system and program product according to Claims 1, 9, 17, wherein: the encrypting data processing system further comprises a client system and a server system coupled for communication, said client system (see Doonan col. 3, lines 9-12: network connected client (sender) and server system) having a client memory device and said server system having an encryption chip and a server memory device:

a) storing the user key further comprises storing the user key in the client memory device; (see Doonan col. 9, lines 44-47: memory area used for data and workspace storage)

b) storing the associated key further comprises storing the associated key in the server memory device; (see Doonan col. 5, lines 4-5: key is stored at server system database)

c) Doonan discloses a check on the validation of a sender's credentials. (see Doonan col. 5, lines 16-20: sender credentials are verified) Doonan does not specifically disclose using a certificate authority (trusted third party) for key validation and determination of key revocation. However, Sudia discloses preventing validation further comprises preventing validation of messages

associated with the user by eliminating the associated key from the server memory device. (see Sudia col. 22, lines 51-63; col. 23, lines 4-7: access revocation list to determinate whether certificate (attached key) is valid)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to invalidate the association key when the status of the association key has been revoked as taught by Sudia. One of ordinary skill in the art would be motivated to employ Sudia in order to enable a trusted third party for a flexible and independent network key management system. (see Sudia col. 10, lines 23-25; col. 11, lines 15-23)

Regarding Claims 6, 14, 22 (currently amended), Doonan discloses the method, system and program product according to Claims 1, 9, 17, further comprising: encrypting the associated key by using an encryption chip key which is stored on an encryption chip of the encrypting data processing system. (see Doonan col. 2, lines 3-8: encryption key transferred to sender system)

Regarding Claims 7, 15, 23 (currently amended), Doonan discloses the method, system and program product according to Claims 6, 14, 22, further comprising: communicating an encrypted associated key to validate the association of the user with the encrypted messages. (see Doonan col. 5, lines 63-67:)

Regarding Claims 8, 16, 24 (original), Doonan discloses the method, system and program product according to Claims 7, 15, 23, further comprising: decrypting the associated key with the encryption chip key. (see Doonan col. 6, lines 1-3)

2. Claims 4, 12, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doonan-Sudia as applied to claims 1, 3 above, and further in view of Cook (US Patent No. 6,732,101).

Regarding Claims 4, 12, 20 (original), Doonan does not disclose a server system to receive, encryption and forward message. However, Cook discloses the method, system and program product according to Claims 3, 11, 19, wherein encrypting the messages further comprises:

a) sending the messages to be encrypted from the client system to the server system; (see Cook col. 2, lines 19-23: send message from client to server for encryption)
b) encrypting the messages using the encryption chip of the server system; (see Cook col. 2, lines 51-55: encrypt message)
c) sending the encrypted messages from the server system to the client system. (see Cook col. 2, lines 51-55: deliver encrypted message to recipient (client) system)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to receive, encrypt and forward a message utilizing any encryption algorithm as taught by Cook. One of ordinary skill in the art

would be motivated to employ Cook in order to enable a flexible and strengthened encryption system. (see Cook col. 2, lines 33-38: " *... Messages can be encrypted using any available encryption means at the sender and sent to a forwarding service. The forwarding service can forward the message to each recipient according to the recipient's decryption capability and preference. ...* ")

3. Claims 5, 13, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Doonan-Sudia-Cook as applied to claims 1, 3, 4 above, and further in view of Marshall (US Patent No. 4,888,800).

Regarding Claims 5, 13, 21 (original), Doonan-Sudia-Cook does not disclose the ability to erase key information after processing of an encrypt message. However, Marshall discloses the method, system and program product according to Claims 4, 12, 20, further comprising: erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system. (see Marshall col. 2, lines 30-35: key information is erased from system)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to erase all key related information after message processing maintaining only current information as taught by Marshall. One of ordinary skill in the art would be motivated to employ Marshall in order to enable a flexible and strengthened network key management system. (see Marshall col. 1, lines 50-58: " *... system has the advantage ... only to maintain the keys required for whatever*

current communication sessions ... a pair of session keys ... every time a link or session is requested ... ")

(10) Response to Argument

As to claims 1, 9, 17, applicant argues in substance that:

A. The referenced prior art does not disclose, teach or suggest the capability for storing an association key in the encrypted data processing system and encrypting the user key with the association key to obtain an encrypted user key and preventing validation of the association of the user with messages by revoking an association key at the encrypting data processing system. (see Appeal Brief Page 6, Lines 29-31)

As to claim 7, applicant argues in substance that:

B. The referenced prior art does not disclose, teach or suggest communicating an encrypted association key to validate the association of the user with the encrypted messages and the combination of cited referenced prior art does not disclose, teach or suggest communication of both an encrypted association key and an encrypted user key. (see Appeal Brief Page 8, Line 7)

Examiner Response to Argument dated November 3, 2005

The examiner's rejection is proper given that the cited passages of Doonan, Sudia,

Cook, and Marshall disclose the applicant's claimed invention.

As to point **A:**

Doonan (6,807,277) not only discloses a client-server encrypted data processing system [see Doonan col. 2, lines 1-13; col. 2, lines 59-61] with storage of key information in the server [see Doonan col. 2, lines 3-7], but also discloses the capability for the encryption of a key itself [see Doonan col. 5, lines 63-67]. Encryption of a key itself in addition to data is well known in the art for the protection of data.

Doonan does not specifically disclose a usage of encryption key pairs and to revoke an encryption key pair. However, Sudia (6,009,177) discloses a server for acquisition of encryption key pairs. Two encryption key pairs, an association key pair and a user key pair, are acquired for each client. [see Sudia col. 15, lines 1-4: *key pair retrieval*] Sudia (6,009,177) also discloses the ability to revoke usage of a particular key pair, by placement of the particular key pair within a certificate revocation list. [see Sudia col. 22, lines 51-63; col. 23, lines 4-7: *software removes authority for client to use a particular key pair as part of the revocation protocol*]

In addition, the applicant's invention defines revoke to be the deletion of an association key pair, which removes an association between a user and a user's key pair thereby removing a user's ability to utilize a particular user's key pair. (see Specification Page 15, Lines 27- 33: *" ... Associated key A may be revoked by simply erasing it from server system **104**. Since associated key A is revoked and no longer exists in server system **104**, the ECK **107** does not have an associated key to decrypt, and encrypted user key 1, in turn, cannot be decrypted since associated key A does not*

exist to decrypt user key 1. ... ") Cook (6,732,101) also discloses the capability to revoke an association key pair by deleting an association encryption key pair. [see Cook col. 6, lines 48-50: *key pair deletion*]

Sudia features combined with Doonan features create one server with the entire set of features. Therefore, the revoke feature is performed at the same data processing system as encryption (i.e. at the encrypting data processing system).

As to point **B:**

Doonan (6,807,277) discloses the ability for encryption of a key itself [see Doonan col. 5, lines 63-67: *encryption of keys*] and communication of that encrypted key with key retrieval information between client and server. [see Doonan col. 2, lines 7-10; col. 2, lines 57-61: *communications of key (i.e. encrypted keys) and key retrieval information (i.e. association key) between client and server*] Key retrieval information is analogous to the association key information, which is used to retrieve and access the user key.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Kyung H. Shin KHS

Jan. 22, 2006

Conferees:

BUNJOB JAROENCHONWANIT
SUPERVISORY PATENT EXAMINER

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100